УДК 323(569.4) : 004.056.5 + 327 : 004.056.5

Г. Н. Валиахметова, Л. В. Цуканов

«СУММА ВСЕХ РЕСУРСОВ СТРАНЫ»: СПЕЦИФИКА ИЗРАИЛЬСКОГО ПОДХОДА К ОБЕСПЕЧЕНИЮ НАЦИОНАЛЬНОЙ КИБЕРБЕЗОПАСНОСТИ

Аннотация. Статья посвящена анализу опыта Государства Израиль в формировании комплексной системы обеспечения национальной кибербезопасности. Авторами рассмотрены ключевые принципы, на которых базируется израильский подход к обеспечению цифровой защиты страны, проанализированы базовые документы, формирующие концептуальную основу израильской политики безопасности в цифровом пространстве. В их числе декларация Д. Бен-Гуриона 1953 г., Национальная стратегия кибербезопасности 2017 г., концепция «кумулятивного сдерживания» и т. д. Раскрыта специфика институциональной структуры национальной кибербезопасности, государственно-частного партнерства и международного сотрудничества как ее базовых элементов. Авторы приходят к выводу, что за последние два десятилетия Израилю удалось разработать комплексный подход к обеспечению безопасности в цифровом пространстве, в рамках которого выстраивается многоуровневая и относительно гибкая система киберзащиты Государства. Отмечается также, что, несмотря на наличие условного «водораздела» между гражданскими и военными сегментами кибербезопасности, а также определенные межведомственные разногласия, ключевые акторы демонстрируют готовность к конструктивному взаимодействию для укрепления национальной устойчивости к угрозам и вызовам цифровой эпохи. Авторы подчеркивают, что сфера кибербезопасности постепенно превращается в ключевой потенциал развития национальной экономики, что, в свою очередь, позволяет прогнозировать в краткосрочной перспективе возможность превращения Израиля в мировой центр высоких технологий и безопасной цифровой среды.

Ключевые слова: Израиль, кибербезопасность, киберугрозы, государственно-частное партнерство, международное сотрудничество

Gulnara N. Valiakhmetova, Leonid V. Tsukanov

“THE SUM OF ALL THE COUNTRY’S RESOURCES”: THE SPECIFICS OF THE ISRAELI APPROACH TO ENSURING NATIONAL CYBERSECURITY

Abstract. The article is devoted to the analysis of the Israeli experience in the field of the formation of an integrated system for ensuring national cybersecurity. The authors considered the key principles on which the Israeli approach to ensuring the digital protection of the country is based, analyzed the basic documents that form the conceptual basis of the Israeli security policy in the digital space. Among them are Ben-Gurion’s 1953 declaration, the National Cybersecurity Strategy2017, the concept of “cumulative deterrence”, etc. The specifics of the institutional structure of national cybersecurity, public-private partnership and international cooperation as its basic elements are disclosed. The authors conclude that over the past two decades, Israel has managed to develop an integrated approach to ensuring security in the digital space, within which a multi-level and relatively flexible system of cyber defense of the State is being built. It is also noted that, despite the existence of a conditional “watershed” between the civilian and military segments of cybersecurity, as well as certain interdepartmental dif-

ferences, key actors demonstrate a readiness for constructive interaction to strengthen national resilience to threats and challenges of the digital age. The authors emphasize that the sphere of cybersecurity is gradually turning into a key potential for the development of the national economy, which, in turn, makes it possible to predict in the short term the possibility of turning Israel into a world center of high technologies and a safe digital environment.
Keywords: Israel, cybersecurity, cyberthreats, public-private partnerships, international cooperation

Рубеж XX–XXI вв. ознаменовался формированием новой – цифровой – реальности, которая, наряду с очевидным улучшением качества жизни человечества, существенно сузила пространство безопасности. Комплекс качественно новых угроз и вызовов поставил в международную повестку вопрос об объединении усилий всех субъектов мировой политики и международных отношений в деле обеспечения надежной защиты глобальной цифровой среды. Однако сложность и противоречивость данного процесса, обусловленная в значительной степени геополитической спецификой постбиполярной эпохи, побуждает государства к выработке собственных подходов и практик защиты национального цифрового пространства. Особый академический и практический интерес представляет уникальный опыт Израиля, который стал предметом многочисленных исследований и дискуссий в научных сообществах США, стран Европы и Азии, однако относительно слабо представлен в российских научных публикациях. Данная статья в определенной степени позволяет восполнить указанный пробел.

Национальная стратегия кибербезопасности Израиля была опубликована в 2017 г. [Prime Minister Office] и стала вторым официальным документом по национальной безопасности после декларации Д. Бен-Гуриона 1953 г. о стратегических принципах. В этом лаконичном документе предпринимается попытка упорядочить ландшафт кибербезопасности страны в контексте корректировки либо пересмотра задач и приоритетов цифровой защиты страны, а также ее институциональных и правовых основ, которые были разработаны в предыдущие два десятилетия. Основные положения Стратегии касаются обеспечения исключительно гражданского сегмента кибербезопасности, который дополняется военной кибероборонной, но не попадает под регулирование Стратегии. Четкое разделение национального пространства на гражданское и военное с точки зрения концепций, институтов, функционала и т. п. является одним из ключевых отличий израильского подхода к обеспечению кибербезопасности.

Согласно Стратегии, гражданская деятельность в сфере кибербезопасности базируется на трех принципах: совокупная прочность, системная устойчивость и национальная оборона. Реализация первого принципа возлагается на частный сектор, который должен обеспечить предприятия и организации технологическими возможностями своевременного обнаружения и парирования киберугроз. В данном сегменте государство поддерживает частный сектор путем установления обязательных стандартов для основных киберпродуктов и услуг, разработки четких инструкций по алгоритму действий в случае чрезвычайных ситуаций, предоставления передовых знаний и опыта для гарантированного преодоления киберугроз. Принцип «системной устойчивости» предполагает способность циф-

ровых систем к быстрому восстановлению после повреждения и реализуется в рамках межведомственного взаимодействия, государственно-частного партнерства и международного сотрудничества. Гражданская «национальная оборона» нацелена на смягчение наиболее серьезных угроз национальной безопасности и обеспечивается исключительно спецслужбами и правоохранительными органами, которые, в свою очередь, взаимодействуют с военными структурами. В случае войны или возникновения чрезвычайных ситуаций Стратегия предусматривает передачу полномочий по регулированию и защите национального цифрового пространства армии в лице Сил обороны Израиля (ЦАХАЛ) [Prime Minister Office].

Стратегия реализуется в рамках различных проектов, в том числе «Высокий замок», «Хрустальный шар», «Витрина», «Кибернет+» и т. д. Все они направлены на решение актуальных проблем цифровой защиты страны и повышение способности Израиля выявлять и предотвращать кибератаки, облегчать обмен информацией между различными участниками системы кибербезопасности [Israel's National Cybersecurity, p. 11–12].

В институциональном плане последнее десятилетие ознаменовалось процессом централизации управленческой структуры гражданского сегмента кибербезопасности страны. С 2018 г. ее ядром является Национальное управление кибербезопасности (*Israel National Cyber Directorate, INCD*), которое сформировалось в результате слияния Национального штаба кибербезопасности (*National Cyber Security Authority, NCSA*), призванного решать оперативные задачи [Even; Matania], и Национального бюро кибербезопасности (*Israel National Cyber Bureau, INCB*), ориентированного преимущественно на политику. *INCD* напрямую подчиняется премьер-министру. Такую подчиненность имеют только три ведомства: Шин Бет (Израильское агентство безопасности, или Шабак), Моссад и Комитет по атомной энергетике, что свидетельствует о значимости зоны ответственности *INCD* общей системе национальной безопасности Израиля. В задачи *INCD* входит разработка и реализация стратегии национальной кибербезопасности, содействие государственно-частному партнерству и международному сотрудничеству в сфере цифровой защиты, определение нормативно-правовых основ деятельности в цифровом пространстве, создание кадрового и инновационного потенциала, координация взаимодействия различных участников киберполитики Израиля [Prime Minister Office]. В 2019 г. бюджет *INCD* составил 64 млн долларов, вдвое превысив показатель предшествующего года [Israel's National Cybersecurity, p. 15].

Ряд гражданских задач кибербезопасности остается вне компетенции *INCD* и относится к зоне ответственности полиции, министерства юстиции и разведслужб (Шин Бет, Моссад и др.). Указанные ведомства зачастую придерживаются иных приоритетных задач и операционных подходов, что приводит к трениям с *INCD*. Так, например, Агентство Шин Бет, которое в течение долгого времени (с 2002 г. до 2012 г., когда был создан *NCSA*) несло ответственность за защиту цифрового пространства на национальном уровне, своим главным приоритетом считает обеспечение безопасности объектов критической инфраструктуры, а не всего гражданского киберпространства. Кроме того, фокусируясь на защите Израиля от внутренних угроз, в том числе с использованием новейших техно-

логий, Шин Бет часто рассматривает гражданские права (конфиденциальность и т. п.) как второстепенные вопросы.

Однако *INCD*, который в своей операционной деятельности в значительной степени вынужден опираться на технический опыт и информацию разведслужб и, соответственно, принимать в расчет их подходы, в рамках своего функционала также призван обеспечивать соблюдение законности и координировать усилия различных ведомств (в том числе внутренней, внешней и военной разведок) в контексте выполнения общенациональных задач [Ibid.].

Отсутствие механизмов надзора, системы сдержек и противовесов, четкой правовой базы деятельности учреждений, связанных с обеспечением кибербезопасности, ставит в общественно-политическую повестку Израиля вопрос о защите демократического процесса. Консолидация властных полномочий в канцелярии премьер-министра в совокупности с готовностью общества поступиться частью своих гражданских прав в обмен на безопасность объективно создает возможности для злоупотреблений политической и кибервластью, нарушений прав человека (например, сбор информации и наблюдение за политической оппозицией или израильтянами исключительно арабского происхождения) [Ibid., p. 15–17]. На уровень общественных дискуссий в Израиле вынесены, кроме того, такие вопросы, как способность компетентных органов устранить риски иностранного вмешательства в избирательные кампании [СМИ: могут ли кибератаки сорвать выборы; Unna, p. 172–173; איך מדינה זרה תתערב בבחירות], обоснованность увеличения расходов на безопасность, в том числе цифровую [Israel's National Cybersecurity, p. 15; תקציב הביטחון יגדל בעוד 1.3 מיליארד שקל], а также в целом эффективность действующей институциональной структуры цифровой защиты страны.

Военные аспекты национальной кибербезопасности находятся в ведении ЦАХАЛа и реализуются двумя его главными организациями – Управлением C4I (отвечает за работу современных средств связи в армии, обеспечивает взаимодействие между разными родами войск, а также устанавливает различные режимы доступа к разным пластам информации и осуществляет постоянный мониторинг с целью предотвращения попыток несанцкционированного доступа в системы внутриармейского интранета как из Израиля, так и из иностранных государств), и Подразделением 8200 (аналог американского Агентства национальной безопасности, АНБ), которое разрабатывает и проводит наступательные кибероперации. Национальная стратегия кибероборонs не представлена в едином официальном документе, но в целом базируется на принципах Д. Бен-Гуриона 1953 г. : сдерживание, решающая победа, раннее предупреждение и альянсы. Оборонительные и наступательные возможности ЦАХАЛа также упомянуты в гражданской Национальной стратегии кибербезопасности 2017 г. и доктрине общественной обороны Г. Эйзенкота 2015 г., которая признает цифровое пространство пятым (после суши, моря, воздуха и космоса) театром военных действий. Другой отличительной особенностью военного сегмента киберзащиты Израиля является конкретная идентификация субъектов угроз, к каковым отнесены Иран, Ливан, Сирия, а также ряд группировок – Хезболла, ХАМАС, ИГИЛ (запрещена в РФ), Палестинский исламский джихад (запрещена в РФ) и т. д. [Eizenkot, p. 4].

В 2012 г. в рамках реализации принципа раннего предупреждения министерство обороны Израиля приступило к разработке проекта «Железный киберкупол». «Каждый день предпринимается большое количество попыток проникнуть в компьютерные системы Израиля, – заявил Б. Нетаньяху, анонсируя проект. – Так же, как у нас есть "Железный купол" для защиты от ракет и террористических ударов, у нас будет аналогичная защита от кибератак» [Netanyahu]. 2012 г. был беспрецедентным по количеству кибератак, жертвами которых в том числе стали авиакомпания *El Al*, Тель-Авивская фондовая биржа, банк *Hapoalim*, а также тысячи израильтян, чьи данные кредитных карт были украдены и размещены в открытом доступе предположительно саудовскими хакерами. О целесообразности и своевременности запуска программы свидетельствует, например, тот факт, что только за первые 4 дня с начала проведения израильской военной операции «Облачный столп» в Секторе Газа в ноябре 2012 г. было совершено 44 млн кибернападений на 700 сайтов правительственных учреждений в рамках твиттер-шторма *#OpIsrael*, инициированного пропалестинским крылом хакерской группировки *Anonymous* [Israel faces 44 million attacks].

ЦАХАЛ также придерживается концепции «кумулятивного сдерживания», которая в том числе предусматривает нанесение ответного удара после пресечения кибератаки [Hochberg L.; Israel's National Cybersecurity, p. 12]. Наглядными примерами «зеркального» ответа могут служить обвал сайтов фондовых бирж в Саудовской Аравии и ОАЭ после указанных выше нападений 2012 г. [Гельман], а также масштабный по своим разрушительным последствиям кибердудар по компьютерным сетям порта Шахид Раджаи (г. Бендер-Аббас) в мае 2020 г. после попытки предположительно иранских хакеров атаковать систему распределения воды в Израиле [Израиль нанес ответный кибердудар; Israeli cyber chief]. Израильская армия, кроме того, создала прецедент, когда в мае 2019 г. в ответ на кибератаку нанесла реальный бомбовый удар по кибер-штабу ХАМАС в Газе [Groll].

Военные кибералъянсы не упоминаются в общедоступных документах, но эксперты предполагают наличие сотрудничества между израильским Подразделением 8200 и американским АНБ, в рамках которого были разработаны первые в мире образцы кибервооружений – вирусные программы *Stuxnet* и *Duqu*, по своей разрушительной мощи сравнимые со стратегическими наступательными вооружениями. Подразделением 8200, также известное как Центральное подразделение сбора данных разведывательного корпуса, подчиняется Управлению военной разведки (АМАН) и сотрудничает с Моссадом и Шин Бет – разведслужбами, не входящими в состав Сил обороны Израиля. Информация, собираемая Подразделением 8200, используется в своей работе всеми израильскими спецслужбами, в т. ч. Службой внешней разведки «Моссад» и Общей службой безопасности Шабак.

После обнаружения в 2012 г. в компьютерных сетях ряда ближневосточных стран вируса *Flame*, представляющего собой высокоточную систему кибершпионажа, ЦАХАЛ признал, что Подразделение 8200 проводит наступательные кибероперации, которые, по мнению экспертов, нацелены на саботаж промышленных объектов, шпионаж и поддержку традиционных вооруженных сил [Israel's National Cybersecurity, p. 15–16].

Специфика израильской стратегии обеспечения национальной цифровой безопасности определяется, помимо выше рассмотренных факторов, активной поддержкой частного бизнеса государством и нацеленностью на укрепление лидерства страны в глобальном киберпространстве, в том числе в технологических, организационных и коммерческих аспектах. «Кибербезопасность растет благодаря сотрудничеству, а кибербезопасность как бизнес огромна, – подчеркивал премьер-министр Израиля Б. Нетаньяху. – Мы потратили огромные средства на нашу военную разведку, а также на Моссад и Шин Бет. Огромная часть этого <…> уходит на кибербезопасность. Мы думаем, что бесконечные поиски безопасности открывают огромные возможности для бизнеса» [цит. по: Ibid., p. 12–13]. В Израиле планомерно создавалась уникальная киберэкосистема, которая базируется на идее обеспечения высокой степени защиты и превосходства за счет инвестиций в человеческий капитал и IT-индустрию, а также сотрудничества правительства, военных ведомств, академических кругов, частных предприятий и иных организаций, имеющих отношение к цифровой среде [Unna, p. 170–171].

Первое партнерство правительства и научных сообществ Израиля осуществлялось в рамках учреждения при поддержке *INCD* Семинара по вопросам науки, технологии и безопасности Юваля Неэмана (2002) и Междисциплинарного центра кибер-исследований им. Блаватника (2014), которые в дальнейшем трансформировались в платформы для неформального обмена знаниями и опытом между представителями частного, государственного, академического и военного секторов [Israel's National Cybersecurity, p. 18].

Весьма успешными проектами государственно-частного сотрудничества в области киберзащиты стали шесть академических исследовательских центров, созданных *INCD* в партнерстве с различными университетами и специализирующихся в разных областях. Показательным примером израильской экосистемы киберинноваций может служить *CyberSpark* в Беэр-Шеве, недалеко от Университета Бен-Гуриона. Там же *INCD* разместил национальный центр *CERT* (команда реагирования на компьютерные чрезвычайные ситуации), который работает в режиме 24/7, оказывая экстренную помощь любому гражданину или организации, ставшим жертвами кибератак. Вслед за правительством и военные ведомства в лице Управления C4I и Подразделения 8200 перенесли в инновационный парк свои важные структуры киберзащиты. Этот проект привлек также и частный капитал, причем не только израильский, но и транснациональный в лице компании *IBM, PayPal, Lockheed Martin, Oracle, Dell, Deutsche Telekom* и т. д. [CyberSpark].

Другую форму государственно-частного партнерства в сфере кибербезопасности демонстрирует пример консорциума израильских компаний *Israel Aerospace Industries (IAI)*, *Check Point* и *El Al*, созданного по инициативе *INCD* с целью разработки и внедрения решений в области цифровой защиты гражданской авиации [Unna, p. 172]. Одним из индикаторов расширения сотрудничества государства, армии и частного сектора являются, кроме того, организационные изменения на крупнейших оборонных предприятиях Израиля (*IAI, Rafael Advanced Defense Systems, Elbit Systems, Israel Military Industries* и т. д.), где с 2013 г. создаются новые киберуправления, возглавляемые, как правило, бывшими офицерами

Подразделения 8200. «Задача оборонной промышленности – сохранить конкурентное преимущество Израиля во всех сферах, а также создать и поддерживать его независимость от иностранных поставщиков», – отмечает Эсти Пешин, основатель и руководитель кибердирекции в *IAI* [цит. по: The Fifth Theater of Battle]. «Мы стремимся предоставить армиям, странам и организациям комплексное решение для критически важной инфраструктуры, – говорит Л. Гроссман, глава киберотдела *Elbit Systems*. – Возможность создать интегрированную систему управления ресурсами в масштабе армии или государства является уникальной особенностью таких компаний, как *Elbit*» [цит. по: Ibid.].

Запуск проекта «Кибернет+» (*CyberNet+*) в январе 2020 г. значительно расширил возможности сотрудничестсва государства и армии с частным сектором, которое, помимо обеспечения киберзащиты, позволяет всем участникам получать важную информацию, коммерческую прибыль или иные «дивиденды». «Кибернет+» представляет собой социальную сеть кластерного типа с элементами нетворкинга, на платформе которой осуществляется безопасный и надежный обмен отчетами и информацией (в том числе анонимной) о кибератаках с целью выявления и киберугроз и противодействия им на ранних стадиях. По сути, «Кибернет+» является постоянно действующей экспертной площадкой, объединяющей около 10 тыс. специалистов – аналитиков, исследователей и менеджеров по информационной безопасности [Israel launches cybersecurity]. Сеть была создана *INCD* в сотрудничестве с лидерами израильской IT-индустрии, а также представителями местных и международных киберсообществ. Израильские эксперты по кибербезопасности дали высокую оценку этой не имеющей аналогов в мире разработке, назвав проект первым практическим шагом к реализации концепции цифрового «Железного купола» [Dennis].

Развитие государственно-частного партнерства способствовало превращению IT-индустрии в мощный сектор экономики Израиля, а самой страны – в международный центр высоких технологий и одного из мировых лидеров в сфере кибербезопасности. Сегодня Израиль располагает комплексной инфраструктурой цифровой защиты, которую формируют частные компании и венчурные фонды, инвестирующие именно в данную область, (например, *Jerusalem Venture Partners Cyber Labs*), а также стартапы и научно-исследовательские проекты, реализующие сотрудничество между высокотехнологическими предприятиями и академическими сообществами.

Значительные инвестиции в инновации и гражданский киберпотенциал, несмотря на проблемы развития экономики, является стратегическим выбором руководства страны. Занимая 31 место в мире по размеру ВВП на душу населения, Израиль расходует на оборону порядка 6–8 % ВВП, для НИОКР этот показатель составляет 4,5 % и в абсолютном выражении является одним из самых высоких в мире. В 2020 г. на долю 420 израильских IT-компаний приходится примерно 20 % мировых венчурных инвестиций (815 млн долларов), а объемы их экспорта составляют порядка 3,8 млрд долларов, или 8 % мирового рынка технологий, обеспечивающих защиту цифровой среды [Israel's National Cybersecurity, p. 8]. 42 израильские компании представлены в мировом рейтинге *Cyber Security Ventures* для 500 ведущих IT-компаний, где занимают второе место, пропуская вперед толь-

ко американских конкурентов [Unna, p. 171]. «Конечное качество любых национальных усилий в области кибербезопасности – это сумма всех ресурсов страны: человеческого капитала, знаний, идей и разработанных технологий, и мы работаем над развитием и расширением возможностей каждого из этих компонентов», – подчеркивает гендиректор *INCD* Игаль Унна [цит. по: Цафрир].

Одним из ключевых элементов системы кибербезопасности является международное сотрудничество. Израиль довольно широко представлен в многосторонних форматах взаимодействия. Он подписал Конвенцию Совета Европы о киберпреступности; входил в состав пятой Группы правительственных экспертов ООН в области информации и телекоммуникаций; в рамках участия в Женевском диалоге по ответственному поведению в киберпространстве внес весомый вклад в разработку соответствующих международно-правовых норм [Israel's National Cybersecurity, p. 8]. Кроме того, Израиль работает в сотрудничестве с более чем 70 киберцентрами экстренной помощи (*CERT*) по всему миру, является участником многочисленных международных форумов, партнером по оказанию цифрового содействия государствам в рамках специализированных программ Всемирного банка, Банка развития Латинской Америки и др. «Чем больше у Израиля связей, тем легче, лучше и эффективнее станет работа по защите и сдерживанию», – считает Игаль Унна [Unna, p. 171].

В сфере кибербезопасности Израиль сотрудничает с целым рядом иностранных государств, а также международных организаций и транснациональных корпораций. Наиболее прочные связи страна установила с военными и киберразведывательными ведомствами США, в первую очередь с АНБ. Израиль первым из государств мира присоединился к курируемой Министерством обороны США программе *Automated Indicator Sharing*, позволяющей государствам оперативно обмениваться информацией о киберугрозах. Основные принципы израильско-американского партнерства в сфере кибербезопасности изложены в Меморандуме о взаимопонимании 2008 г. и Декларации о цифровой защите 2016 г. [Israel's National Cybersecurity, p. 5, 18].

Несмотря на весьма ограниченный объем информации относительно взаимодействия израильских спецслужб с зарубежными коллегами, все же представляется возможным сделать вывод об их значительном вкладе в обеспечение безопасной цифровой среды по всему миру. Так, например, в 2013 г. Даниэль Коэн-Ор, профессор Тель-Авивского университета и один из ведущих израильских IT-экспертов, был удостоен Ордена Дружбы – высшей награды Китайской Народной Республики для иностранцев [Prof. Daniel Cohen-Or]. Как известно, на мировой арене Израиль с большим отрывом лидирует в области использования новейших ИКТ в противодействии террористическим угрозам, прежде всего со стороны так называемых «волков-одиночек». Прокатившаяся по Европе в 2015–2016 гг. волна терактов побудила Великобританию, ряд стран Евросоюза и Европол активизировать усилия по обмену опытом с израильскими киберподразделениями [Карасова, с. 16]. В 2017 г., после предотвращения израильскими спецслужбами крупного теракта на эмиратском авиалайнере, совершавшем рейс из Сиднея в Абу-Даби, правительство Австралии подписало с Израилем Меморандум о взаимопонима-

нии и сотрудничестве в сфере кибербезопасности [PM signs cyber security MoU]. «Наша система кибербезопасности предотвратила 50 террористических атак по всему миру», – заявил Б. Нетаньяху на открытии VIII международной конференции *CyberTech* в Тель-Авиве в 2019 г. [цит. по: Гельман].

На совместное противодействие терроризму, в том числе с применением качественно новых информационно-аналитических технологий и сервисов, нацелено межведомственное соглашение, подписанное финансовыми разведками Израиля и России 30 июня 2005 г. [Росфинмониторинг]. Взаимодействие двух стран, однако, время от времени осложняется императивами «высокой» политики. Так, в 2018 г. в американский санкционный список попал ряд российских IT-компаний, а также две израильские (*Embedi* и *Erpscan*, в последней также представлен чешский и голландский капитал), которые, по информации Министерства финансов США, сотрудничали с российской консалтинговой компанией *Digital Security* [Гельман].

В последнее десятилетие важными форматами международного взаимодействия Израиля в цифровой области также стали ежегодные профильные конференции (*Cybertech*, *Cyber Week* и т. д.), на которых собираются лидеры израильской и мировой IT-индустрии из более чем 80 стран для обсуждения актуальных проблем кибербезопасности. Еще одна цель подобных форумов, которые проводятся при финансовой поддержке *INCD* и МИД Израиля, – развитие киберкультуры и повышение осведомленности израильской общественности в вопросах защиты от киберугроз. Реализация указанной цели осуществляется, кроме того, в рамках государственно-частного партнерства и развития специализированных образовательных программ.

С 2011 г. *INCB,* а затем его преемник *INCD* совместно с ЦАХАЛ и Министерством образования последовательно и поэтапно разрабатывало и запускало систему цифрового образования и просвещения, уделяя особое внимание молодому поколению израильтян. В школьные образовательные стандарты, начиная с 4 класса, включено программирование, а ученики старшей школы, проявившие способности к изучению точных наук, имеют возможность освоить технологии шифрования и методы противодействия хакерским атакам [Гельман]. Значительная работа по выявлению и обучению талантливой молодежи 16–18 лет проводится, кроме того, в рамках внешкольных образовательных курсов – *Magshimim Le'umit* и *Nitzanei Magshimim*, 75 % их выпускников в дальнейшем служат в кибер- и разведывательных подразделениях ЦАХАЛа), а также программы *Gvahim,* которая готовит учащихся к вступительным экзаменам в университеты по кибербезопасности, информатике и математике [Israel starts training teenagers; Kfir].

Подготовка военнослужащих для киберподразделений осуществляется и финансируется военным ведомством и предусматривает две траектории. Первая позволяет получить высшее инженерное образование при условии увеличения до 5 лет сроков последующей обязательной службы в ЦАХАЛ. Вторая программа (*Talpiot*) проводится Управлением оборонных исследований и разработок и нацелена на элитную киберподготовку одаренных выпускников школ в течение 40 месяцев. По окончании службы в армии такие специалисты, как правило, успешно находят работу в частных *IT*-компаниях, где продолжают совершенствовать свои

профессиональные навыки, оставаясь резервистами ЦАХАЛ до 40–50 лет [Israel's National Cybersecurity, p. 16, 18].

Таким образом, Израиль разработал комплексный подход к обеспечению кибербезопасности, в рамках которого выстраивается многоуровневая система цифровой защиты страны. Руководство страны продемонстрировало политическую волю и приложило значительные усилия для централизации управления и координации действий всех субъектов цифровой безопасности – правительственных ведомств, военных и разведывательных структур, частных компаний и иных заинтересованных сторон. Все они, несмотря на институциональное разделение военной и гражданской кибербезопасности, а также определенные межведомственные разногласия, демонстрируют готовность к конструктивному взаимодействию для укрепления национальной устойчивости к угрозам и вызовам цифровой эпохи. Кроме того, сфера кибербезопасности, аккумулировав усилия государства и общества, трансформировалась в ключевой потенциал для развития человеческого капитала и инновационно-ориентированной экономики, а также для превращения Израиля в мировой центр высоких технологий и безопасной цифровой среды.

Список литературы

Гельман З. Кибербезопасность по-израильски // Независимое военное обозрение. 27.09.2019. URL: https://nvo.ng.ru/armament/2019–09–27/1_1063_israel.html (дата обращения: 10.02.2021).

Израиль нанес ответный кибердар по иранскому морскому порту // Eurasia Daily. 19.05.2020. URL: https://eadaily.com/ru/news/2020/05/19/wp-izrail-nanyos-otvetnyy-kiberudar-po-iranskomu-morskomu-portu (дата обращения: 10.02.2021).

Карасова Т. А., Маген Ц., Швейцер Й. Угрозы глобализации ближневосточного терроризма: взгляд из России и Израиля. Доклад Международного дискуссионного клуба «Валдай». Москва, октябрь 2016. URL: http://ru.valdaiclub.com/files/14052/ (дата обращения: 12.02.2021).

Росфинмониторинг. Межведомственные соглашения. URL: http://www.fedsfm.ru/activity/bilateral-interagency-agreements (дата обращения: 10.03.2021).

СМИ: могут ли кибератаки сорвать выборы в Израиле // Cursor Info. 18.03.2021. URL: https://cursorinfo.co.il/israel-news/smi-mogut-li-kiberataki-sorvat-vybory-v-izraile/ (дата обращения: 20.03.2021).

Цафрир Дж. Три направления деятельности израильского Кибер-директората: Интервью с Игалем Унна // Посольство Израиля в Беларуси. 8.02.2018. URL: https://embassies.gov.il/minsk/NewsAndEvents/Pages/Cyber_directorate.aspx (дата обращения: 15.03.2021).

CyberSpark [website], URL: http://cyberspark.org.il/ (mode of access: 20.03.2021)

Dennis G. Cybernet: A New Israeli Cybersecurity Social Network // VNP Overview. 20.01.2020. URL: https://vpnoverview.com/news/cybernet-a-new-israeli-cybersecurity-social-network/ (mode of access: 20.03.2021).

Eizenkot G. Deterring Terror. How Israel Confronts the Next Generation of Threats. English Translation of the Official Strategy of the Israel Defense Forces. Belfer Center Special Report. 2016. URL: https://www.belfercenter.org/sites/default/files/legacy/files/IDF%20doctrine%20translation%20-%20web%20final2.pdf (mode of access: 01.03.2021).

Even S., Siman-Tov D., Siboni G. Structuring Israel's Cyber Defense // INSS. 21.09.2016. URL: https://www.inss.org.il/publication/structuring-israels-cyber-defense/ (mode of access: 20.03.2021).

Groll E. The Future Is Here, and It Features Hackers Getting Bombed // Foreign Policy. 6.05.2019. URL: https://foreignpolicy.com/2019/05/06/the-future-is-here-and-it-features-hackers-getting-bombed/ (mode of access: 12.03.2021).

Hochberg L., Campbell E. The Potential Cyber Consequences of Israeli Annexation of Palestinian Territory // Middle East Institute. 20.07.2020. URL: https://www.mei.edu/publications/potential-cyber-

consequences-israeli-annexation-palestinian-territory (mode of access: 10.03.2021).

Israel Faces 44 Million Attacks on Websites In Response to Gaza Offensive // Russia Today. 18.11.2012. URL: https://www.rt.com/news/israel-cyber-hackers-gaza-000/ (mode of access: 20.03.2021).

Israel Launches Cybersecurity Social Network 'Cybernet' // Express Computer. 20.01.2020. URL: https://www.expresscomputer.in/security/israel-launches-cybersecurity-social-network-cybernet/45575/ (mode of access: 20.03.2021).

Israel Starts Training Teenagers to Create 'Digital Iron Dome' // The Verge. 02.01.2013. URL: https://www.theverge.com/2013/1/2/3827008/israel-educates-teenagers-in-cyberwarfare-to-create-digital-iron-dome (mode of access: 20.03.2021).

Israel's National Cybersecurity and Cyberdefense Posture: Policy and Organizations. Cyberdefense Report. Zürich: Center for Security Studies, September 2020. URL: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020–09-Israel (mode of access: 10.02.2021).

Israeli Cyber Chief: Major Attack On Water Systems Thwarted // Associated Press. 28.05.2020. URL: https://apnews.com/article/63c081ec091f4c1e3f438ee35243efe0 (mode of access: 20.03.2021).

Kfir I. Learning From Israel's Cyber Playbook // Asia & the Pacific Policy Society, 5.11.2018. URL: https://www.policyforum.net/learning-israels-cyber-playbook/ (mode of access: 20.03.2021).

Matania E., Yoffe L., Goldstein T. Structuring the National Cyber Defence: In Evolution Towards a Central Cyber Authority // Journal of Cyber Policy. 2017. № 1. Pp. 19–25.

Netanyahu: Israel under Cyber Attack from Iran // Xinhua. 15.10.2012. URL: http://www.china.org.cn/world/2012–10/15/content_26790689.htm (mode of access: 20.03.2021).

PM Signs Cyber Security MoU with Israel // Australia Defence Magazine. 01.11.2017. URL: https://www.australiandefence.com.au/defence/cyber-space/pm-signs-cyber-security-mou-with-israel (mode of access: 10.02.2021).

Prime Minister Office. Israel National Cyber Security Strategy in Brief. September 2017. URL: https://cyber.haifa.ac.il/images/pdf/cyber_english_A5_final.pdf (mode of access: 10.03.2021).

Prof. Daniel Cohen-Or [website]. URL: https://www.cs.tau.ac.il/~dcor/ (mode of access: 20.03.2021).

The Fifth Theater of Battle: Cyberwar // Haaretz. 14.01.2014. URL: https://www.haaretz.com/israel-news/business/.premium-the-5th-theater-of-battle-cyberwar-1.5311115 (mode of access: 20.03.2021).

Unna Y. National Cyber Security in Israel // Cyber, Intelligence, and Security. Vol. 3. No. 1, May 2019. Pp. 167–173.

?איך מדינה זרה תתערב בבחירות (Эйх медина зара титарев бе'бхирот?) [Как иностранное государство вмешается в выборы?] // Israel Hayom. 27.07.2019. URL: https://www.israelhayom. co.il/article/623223 (mode of access: 18/02.2021).

תקציב הביטחון יגדל בעוד 1.3 מיליארד שקל (Такциб ха'битахон йигдаль беод 1,3 мильярд шеккель) [Военный бюджет увеличится еще на 1,3 млрд шекелей] // Calcalist. 26.11.2018. URL: https://www.calcalist. co.il/local/articles/0,7340, L 3750608,00.html (mode of access: 18.02.2021).

References

CyberSpark [website]. URL: http://cyberspark.org.il/ (mode of access: 20.03.2021)

Dennis, G. (2020). Cybernet: A New Israeli Cybersecurity Social Network. In *VNP Overview*. 20.01.2020. URL: https://vpnoverview.com/news/cybernet-a-new-israeli-cybersecurity-social-network/ (mode of access: 20.03.2021).

?איך מדינה זרה תתערב בבחירות (Eih medina zara titarev be'bhirot?) [How Will a Foreign State Interfere in the Elections?]. In *Israel Hayom*. 27.07.2019. URL: https://www.israelhayom.co.il/article/623223 (mode of access: 18.02.2021).

Eizenkot, G. (2016). *Deterring Terror. How Israel Confronts the Next Generation of Threats*. English Translation of the Official Strategy of the Israel Defense Forces. Belfer Center Special Report. URL: https://www.belfercenter.org/sites/default/files/legacy/files/IDF%20doctrine%20translation%20-%20web%20final2.pdf (mode of access: 01.03.2021).

Even, S., Siman-Tov, D., Siboni, G. (2016). Structuring Israel's Cyber Defense. In *INSS*. 21.09.2016. URL: https://www.inss.org.il/publication/structuring-israels-cyber-defense/ (mode of access: 20.03.2021).

Gel'man, Z. (2019). Kiberbezopasnost' po-izrail'ski [Cybersecurity in israeli]. In *Nezavisimoe voennoe obozrenie*. 27.09.2019. URL: https://nvo.ng.ru/armament/2019–09–27/1_1063_israel.html (mode of access: 10.02.2021).

Groll, E. (2019). The Future Is Here, and It Features Hackers Getting Bombed. In *Foreign Policy*. 6.05.2019. URL: https://foreignpolicy.com/2019/05/06/the-future-is-here-and-it-features-hackers-getting-

bombed/ (mode of access: 12.03.2021).

Hochberg, L., Campbell, E. (2020). The Potential Cyber Consequences of Israeli Annexation of Palestinian Territory. In *Middle East Institute*. 20.07.2020. URL: https://www.mei.edu/publications/potential-cyber-consequences-israeli-annexation-palestinian-territory (mode of access: 10.03.2021).

Israel Faces 44 Million Attacks on Websites In Response to Gaza Offensive. In *Russia Today*. 18.11.2012. URL: https://www.rt.com/news/israel-cyber-hackers-gaza-000/ (mode of access: 20.03.2021).

Israel Launches Cybersecurity Social Network 'Cybernet'. In *Express Computer*. 20.01.2020. URL: https://www.expresscomputer.in/security/israel-launches-cybersecurity-social-network-cybernet/45575/ (mode of access: 20.03.2021).

Israel Starts Training Teenagers to Create 'Digital Iron Dome'. In *The Verge*. 02.01.2013. URL: https://www.theverge.com/2013/1/2/3827008/israel-educates-teenagers-in-cyberwarfare-to-create-digital-iron-dome (mode of access: 20.03.2021).

Israel's National Cybersecurity and Cyberdefense Posture: Policy and Organizations. Cyberdefense Report. Zürich: Center for Security Studies, September 2020. URL: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020–09-Israel (mode of access: 10.02.2021).

Israeli Cyber Chief: Major Attack On Water Systems Thwarted. In *Associated Press*. 28.05.2020. URL: https://apnews.com/article/63c081ec091f4c1e3f438ee35243efe0 (mode of access: 20.03.2021).

Izrail' nanes otvetnyi kiberudar po iranskomu morskomu portu [Israel retaliates cyber attack on Iranian seaport]. In *Eurasia Daily*. 19.05.2020. URL: https://eadaily.com/ru/news/2020/05/19/wp-izrail-nanyos-otvetnyy-kiberudar-po-iranskomu-morskomu-portu (mode of access: 10.02.2021).

Karasova, T. A., Magen, Ts., Shveitser, I. (2016). *Ugrozy globalizatsii blizhnevostochnogo terrorizma: vzgliad iz Rossii i Izrailia* [Threats of Globalization of Middle East Terrorism: A View from Russia and Israel]. Doklad Mezhdunarodnogo diskussionnogo kluba "Valdai'. Moskva, oktiabr' 2016. URL: http://ru.valdaiclub.com/files/14052/ (mode of access: 12.02.2021).

Kfir, I. (2018). Learning From Israel's Cyber Playbook. In *Asia & the Pacific Policy Society*, 5.11.2018. URL: https://www.policyforum.net/learning-israels-cyber-playbook/ (mode of access: 20.03.2021).

Matania, E., Yoffe, L., Goldstein, T. (2017). Structuring the National Cyber Defence: Evolution Towards a Central Cyber Authority. In *Journal of Cyber Policy*. 2017. No. 1, pp. 19–25.

Netanyahu: Israel under Cyber Attack from Iran. In *Xinhua*. 15.10.2012. URL: http://www.china.org.cn/world/2012–10/15/content_26790689.htm (mode of access: 20.03.2021).

PM Signs Cyber Security MoU with Israel. In *Australia Defence Magazine*. 01.11.2017. URL: https://www.australiandefence.com.au/defence/cyber-space/pm-signs-cyber-security-mou-with-israel (mode of access: 10.02.2021).

Prime Minister Office. *Israel National Cyber Security Strategy in Brief*. September 2017. URL: https://cyber.haifa.ac.il/images/pdf/cyber_english_A5_final.pdf (mode of access: 10.03.2021).

Prof. Daniel Cohen-Or [website]. URL: https://www.cs.tau.ac.il/~dcor/ (mode of access: 20.03.2021).

Rosfinmonitoring. Mezhvedomstvennye soglasheniia [Rosfinmonitoring. Interdepartmental agreements]. URL: http://www.fedsfm.ru/activity/bilateral-interagency-agreements (mode of access: 10.03.2021).

SMI: mogut li kiberataki sorvat' vybory v Izraile [Media: can cyberattacks disrupt Israeli elections]. In *Cursor Info*. 18.03.2021. URL: https://cursorinfo.co.il/israel-news/smi-mogut-li-kiberataki-sorvat-vybory-v-izraile/ (mode of access: 20.03.2021).

The Fifth Theater of Battle: Cyberwar. In *Haaretz*. 14.01.2014. URL: https://www.haaretz.com/israel-news/business/.premium-the-5th-theater-of-battle-cyberwar-1.5311115 (mode of access: 20.03.2021).

תקציב הביטחון יגדל בעוד 1.3 מיליארד שקל (Takziv ha'bitahon yigdal beod 1.3 milliard sheqel) [The Military Budget Will Increase by another 1.3 Billion Shekels]. In *Calcalist*. 26.11.2018. URL: https://www.calcalist.co.il/local/articles/0,7340,L-3750608,00.html (mode of access: 18.02.2021).

Tsafrir, Dzh. (2018). Tri napravleniia deiatel'nosti izrail'skogo Kiber-direktorata: Interv'iu s Igalem Unna [Israel's Cyber Directorate's three activities: Interview with Yigal Unna]. In *Posol'stvo Izrailia v Belarusi*. 8.02.2018. URL: https://embassies.gov.il/minsk/NewsAndEvents/Pages/Cyber_directorate.aspx (data mode of access: 15.03.2021).

Unna, Y. (2019). National Cyber Security in Israe. In *Cyber, Intelligence, and Security*. Vol. 3. No. 1, pp. 167–173.

The article was submitted on 5.04.2021